Capstone Final Report- PGPCS-UTA June 2023
<Wenshan, Liu>

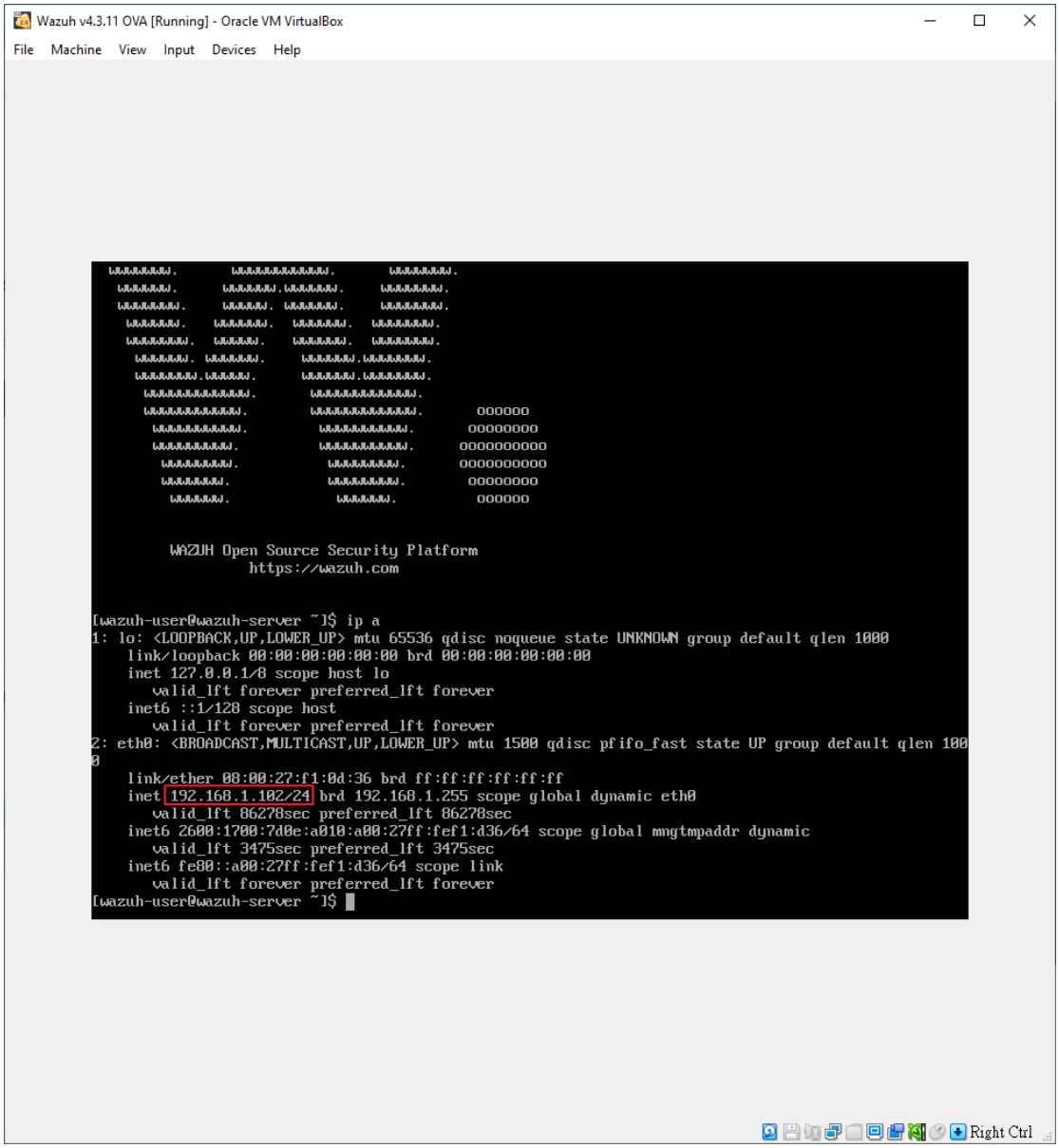
Objectives completed:

- Task 1 – Wazuh Installation and Configuration
- Task 2 – Wazuh Agent Installation and Configuration
- Task 3 – Acquiring Authentication Failure Logs
- Task 4 – Generating report for Authentication Failure Logs
- Task 5 – Setting Up Wazuh File Integrity Monitoring
- Task 6 – Generating Report for File Integrity Management
- Task 7 – Detecting Vulnerabilities in Windows Machine
- Task 8 – Analyzing the Vulnerability Dashboard

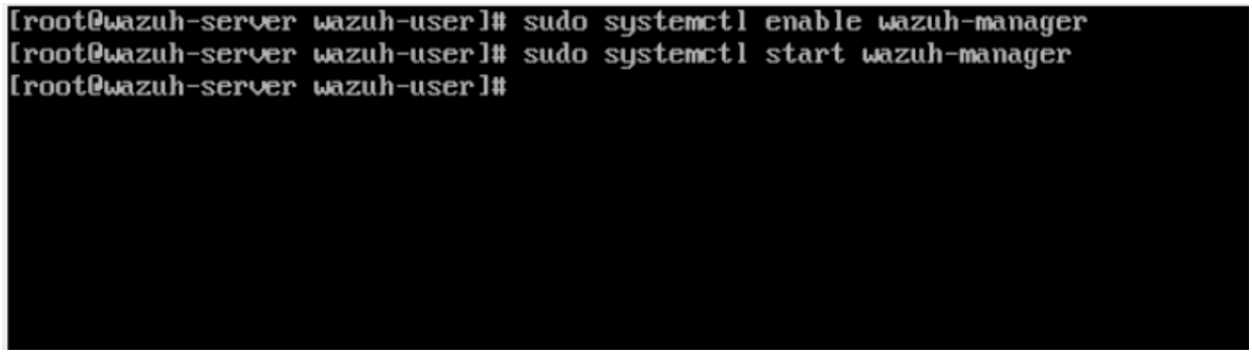
Implementation:

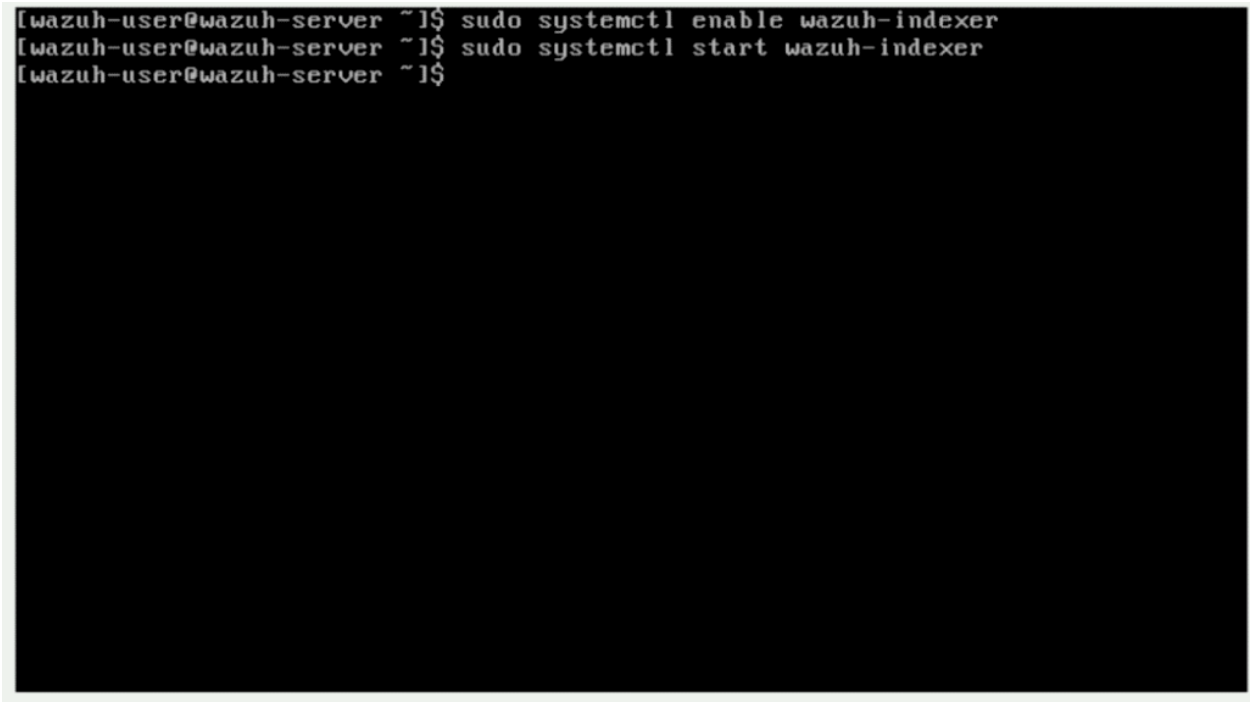
- Task 1 – Wazuh Installation and Configuration

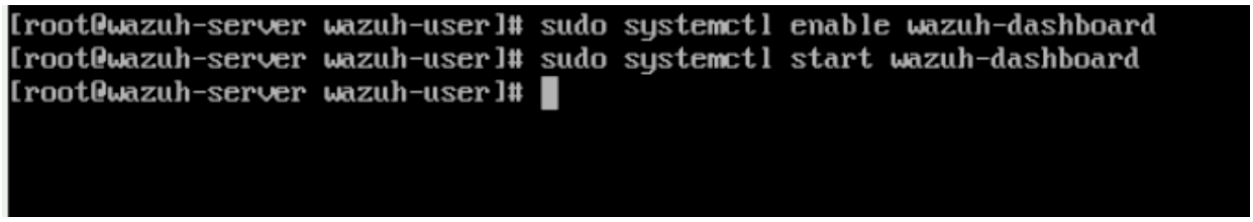
In this task, the Wazuh server would be installed on a Linux system. Here is a screenshot of the successful installation. At the same time, check the IP address, and this machine will be investigated later.



To make sure the server can work appropriately. The services should be started with root user privilege. Thus, use the command **“sudo su”** and enter the password for Wazuh-user as wazuh.

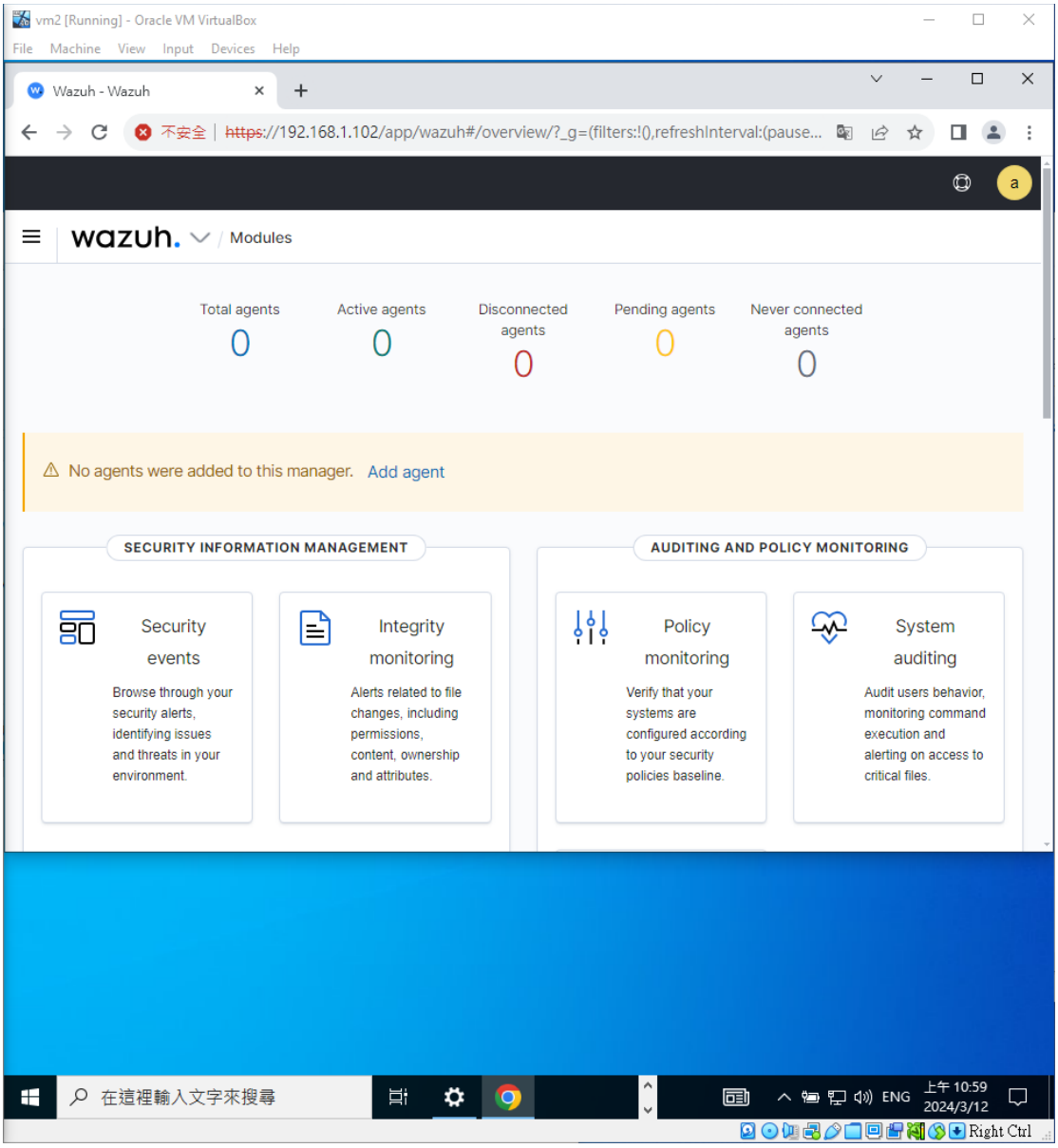






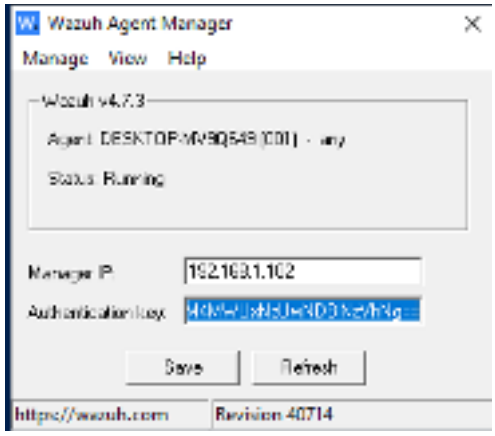
Ensure that the service is working. The command "systemctl" may verify this.

Next, power on the Windows machine and enter the IP of the Linux machine on the Wazuh server in the web browser. Here is a screenshot of logging in successfully.

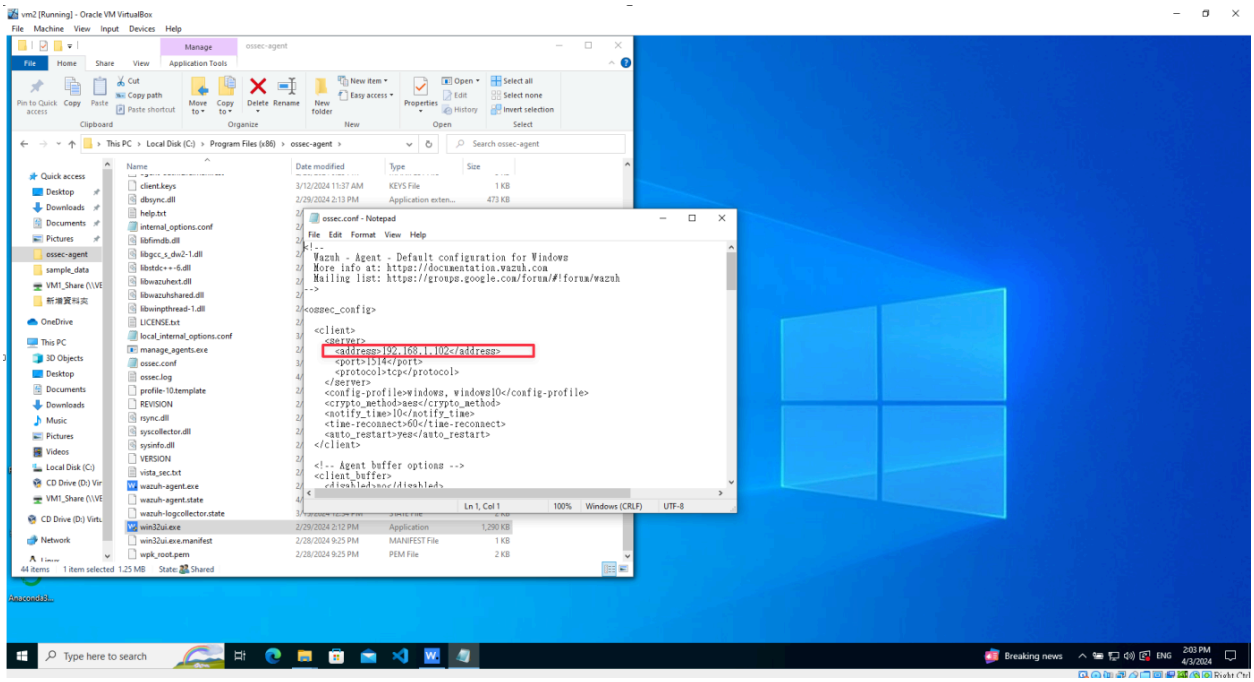


- Task 2 – Wazuh Agent Installation and Configuration

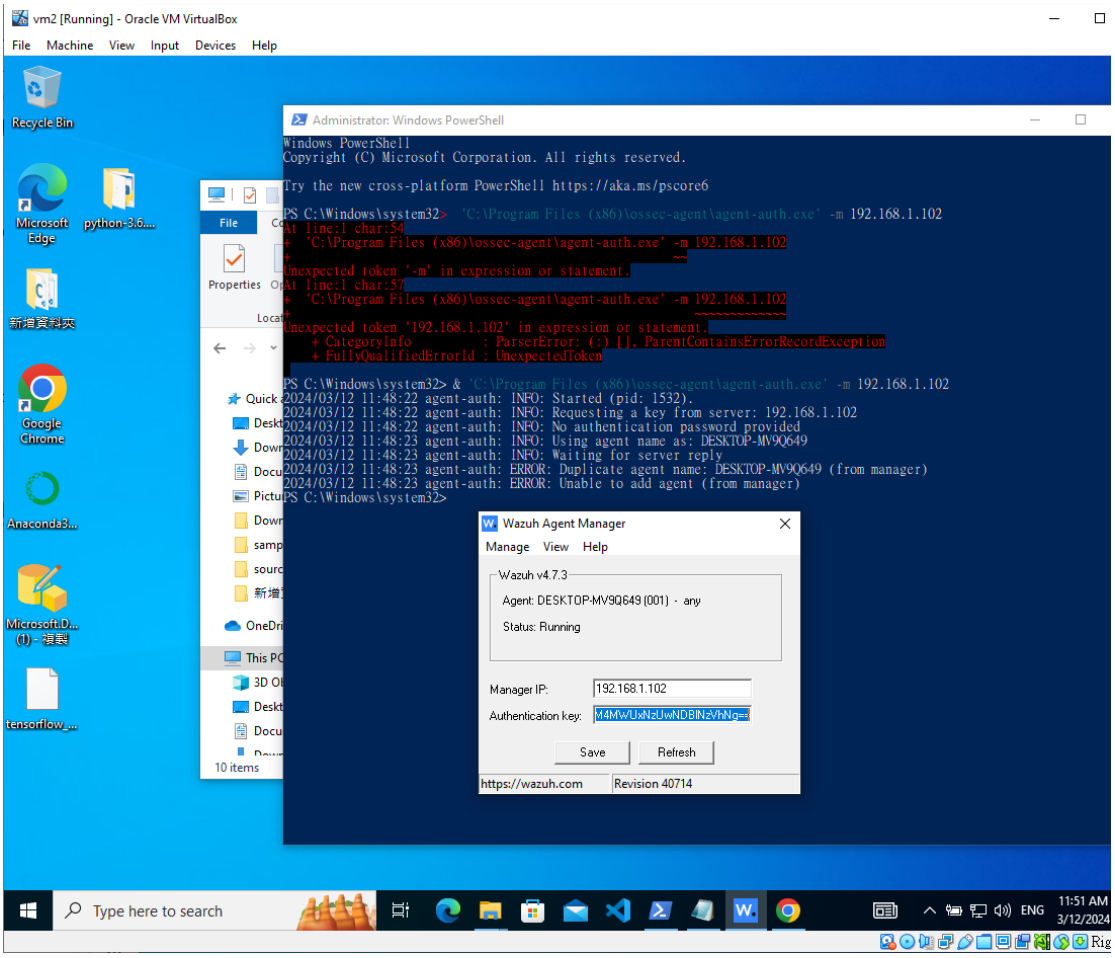
In task 2, the Wazuh agent would be installed on the Windows machine. Download and install wazuh-agent4.3.10-1.msi. After installed, open Win32ui.exe in C Drive> Program Files (X86) > ossec-agent path.



Next step, go to “View” -> “View Config” to adjust Wazuh’s IP address as seen in the Wazuh CLI.

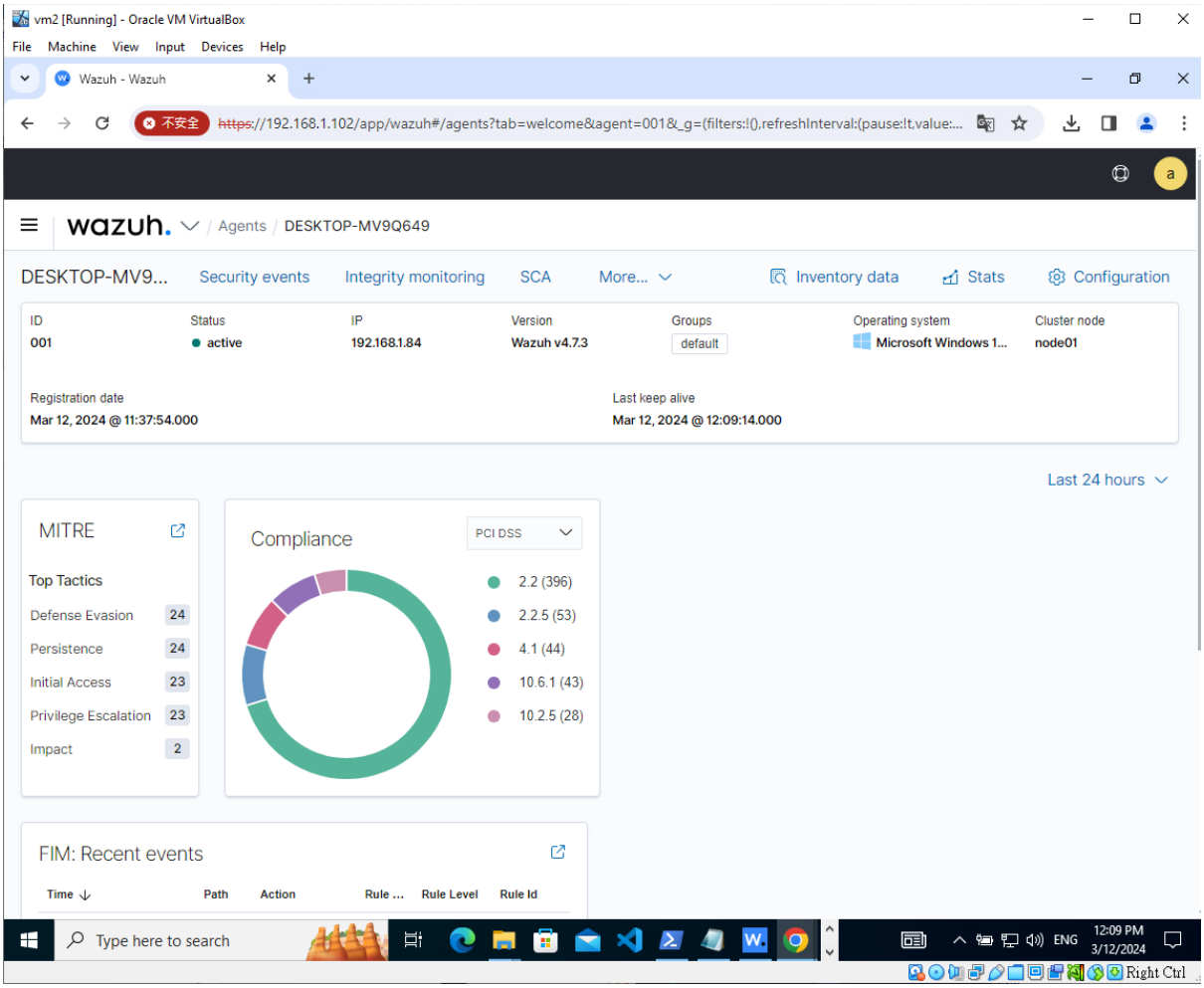


Open Windows PowerShell to get a valid key. Command: “& ‘C:\Program Files (x86)\ossec-agent\agent-auth.exe' -m <IP_ADDRESS_OF_WAZUH> “



Then, go to ‘Wazuh Agent Manager'-> ‘Manage’ -> ‘Start.’ In this step, it would restart the agent after a change.

Go to Wazuh Dashboard to verify the agent was added.

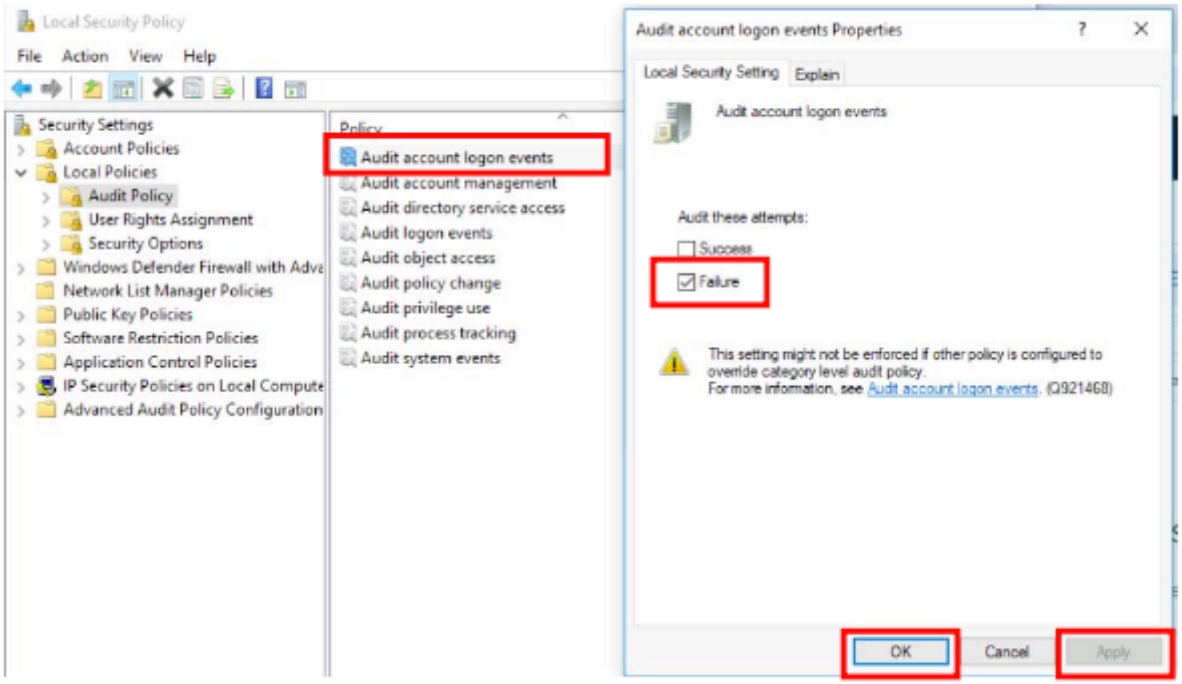


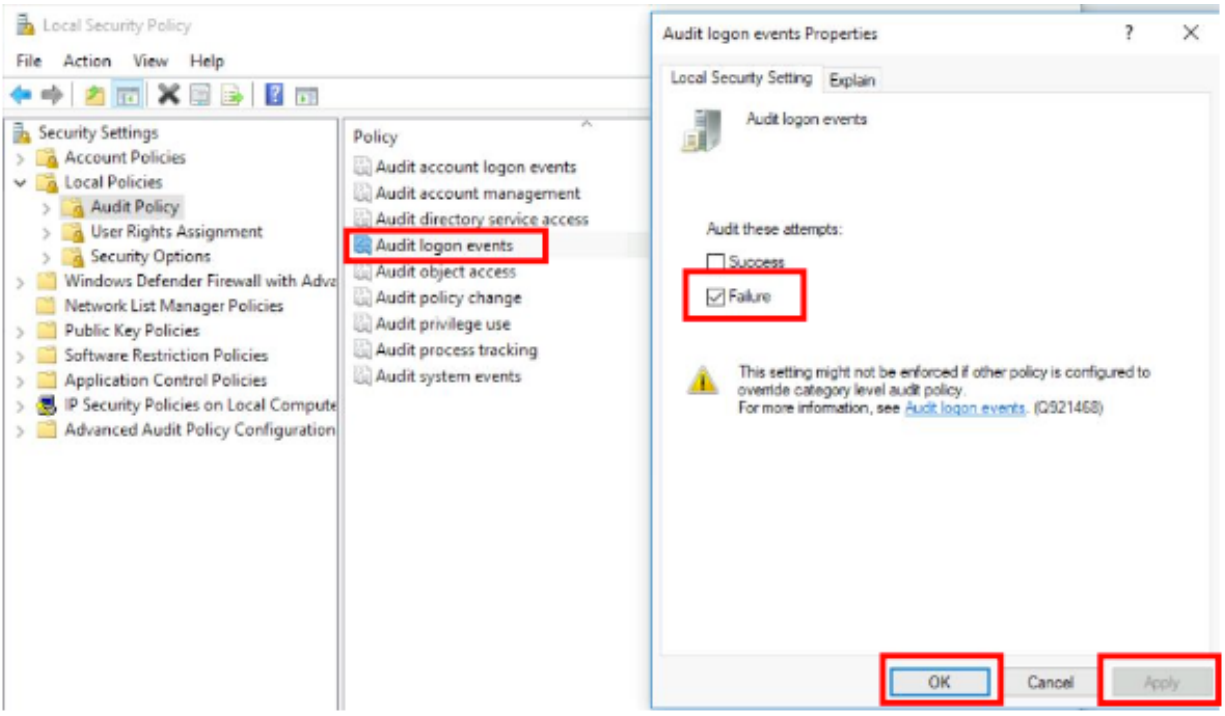
- Task 3 – Acquiring Authentication Failure Logs

  In this task, I will give an example of how to get the authentication failure logs.

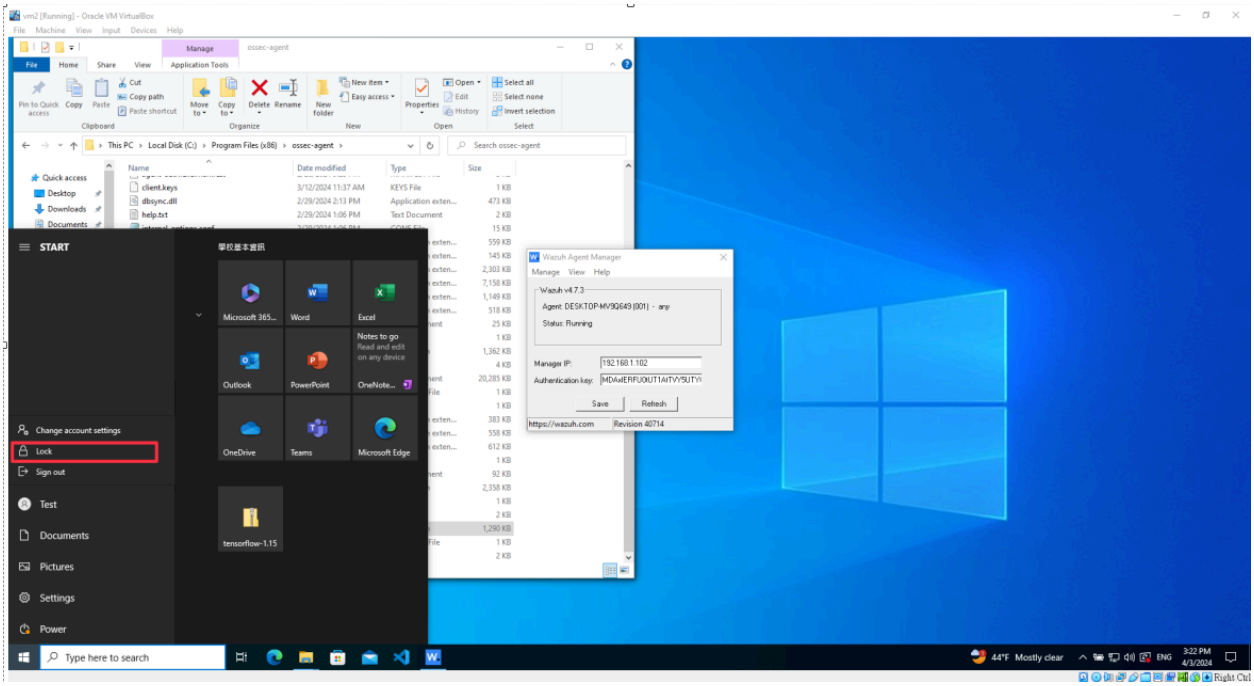
  Firstly, on the Windows machine, go to ‘Local Security Policy’ -> ‘Local Policies’ -> ’Audit Policy’ ->'Audit account logon events’ -> click ‘Failure’ -> and click ‘Apply’ and ‘OK’.

  Secondly, go to ‘Local Security Policy’ -> ‘Local Policies’ -> ‘Audit account logon events.
  ’->'Audit logon events’ -> click 'Failure', then click ‘Apply’ and ‘OK’.

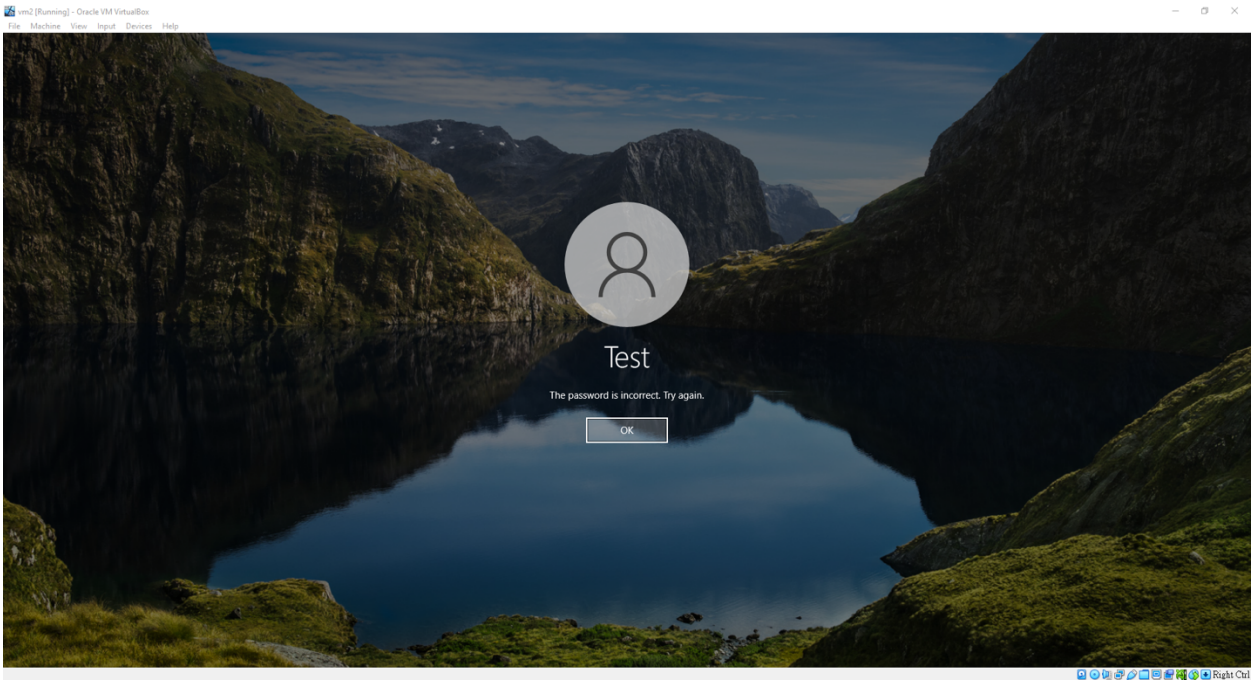




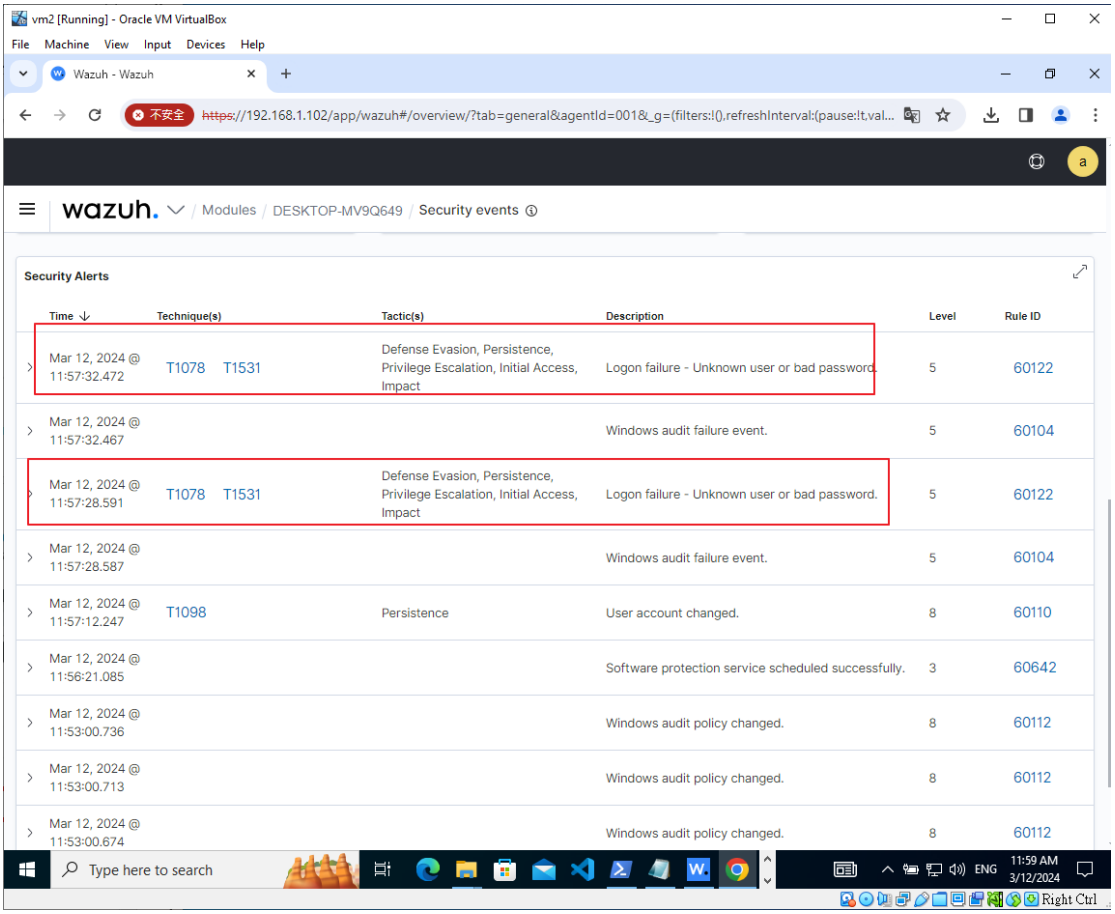
Third, lock the windows machine.



Try logging via incorrect passwords many times.



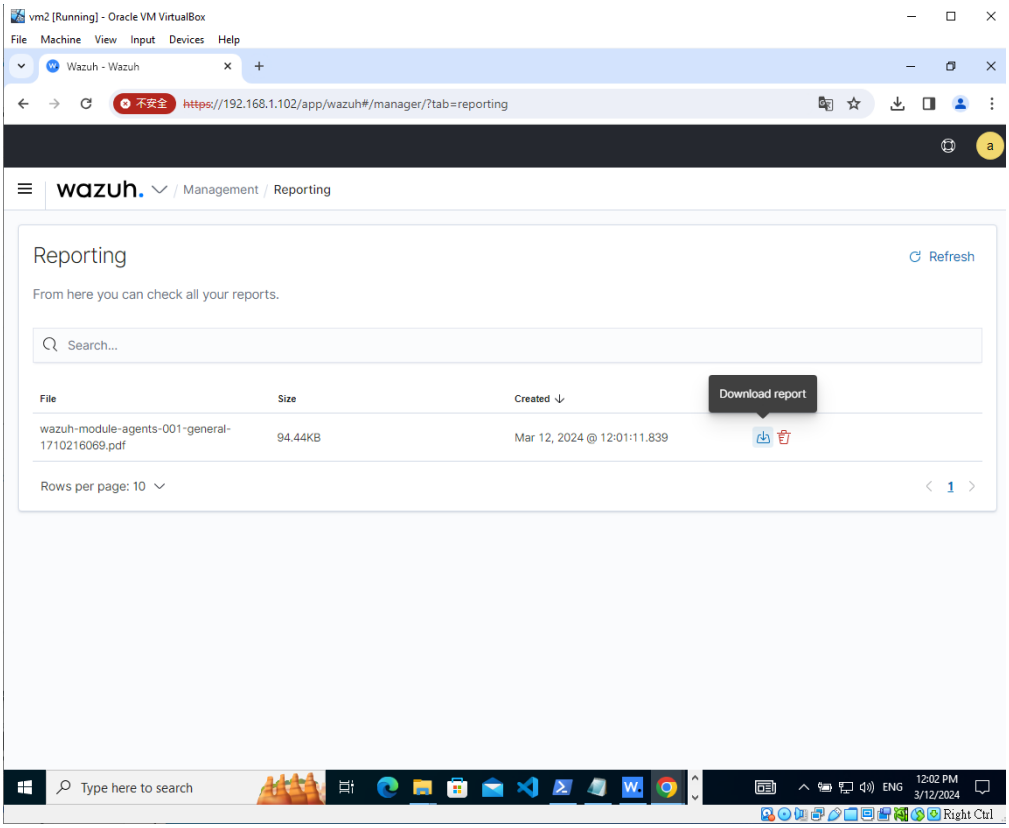
Finally, go to the Wazuh dashboard and click on "security events." The picture below displays the authentication failure logs.

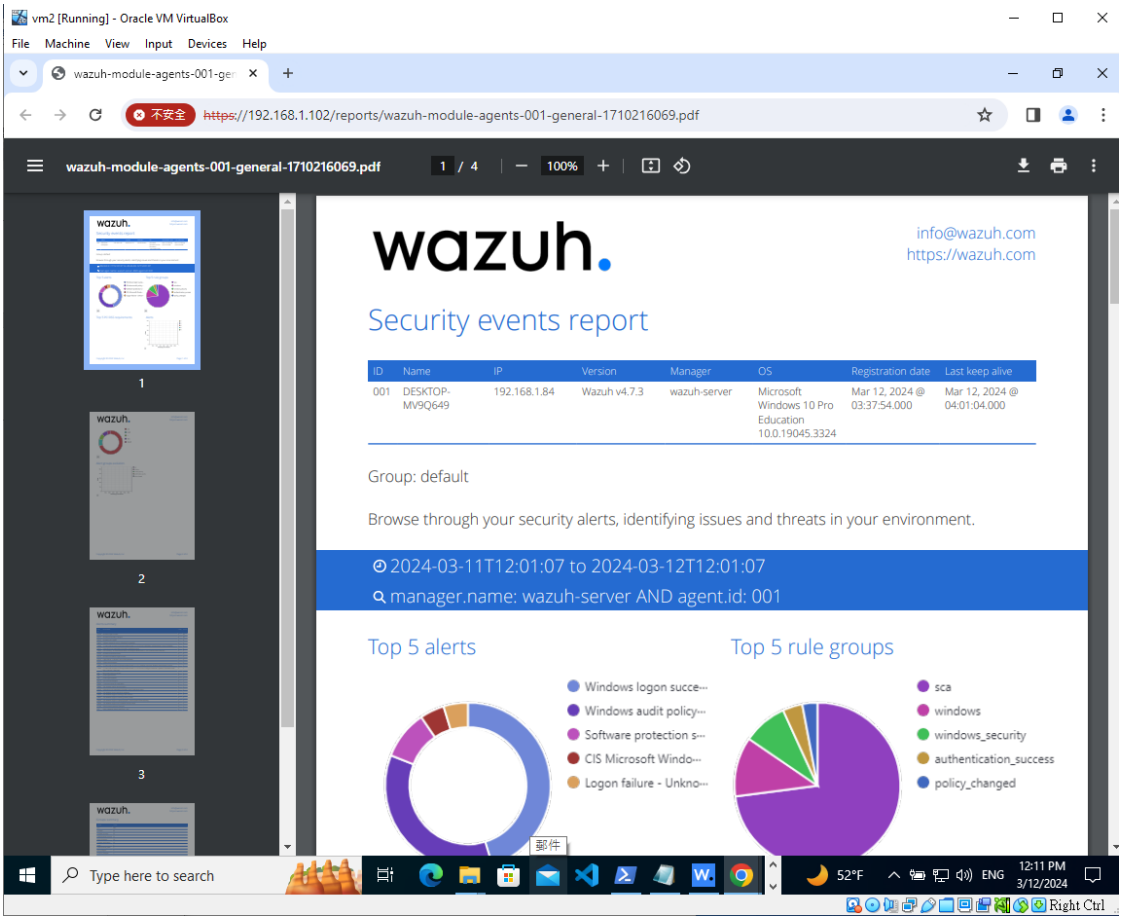


- Task 4 – Generating report for Authentication Failure Logs

  In this task, it is an example of how to generate reports for authentication failure logs.

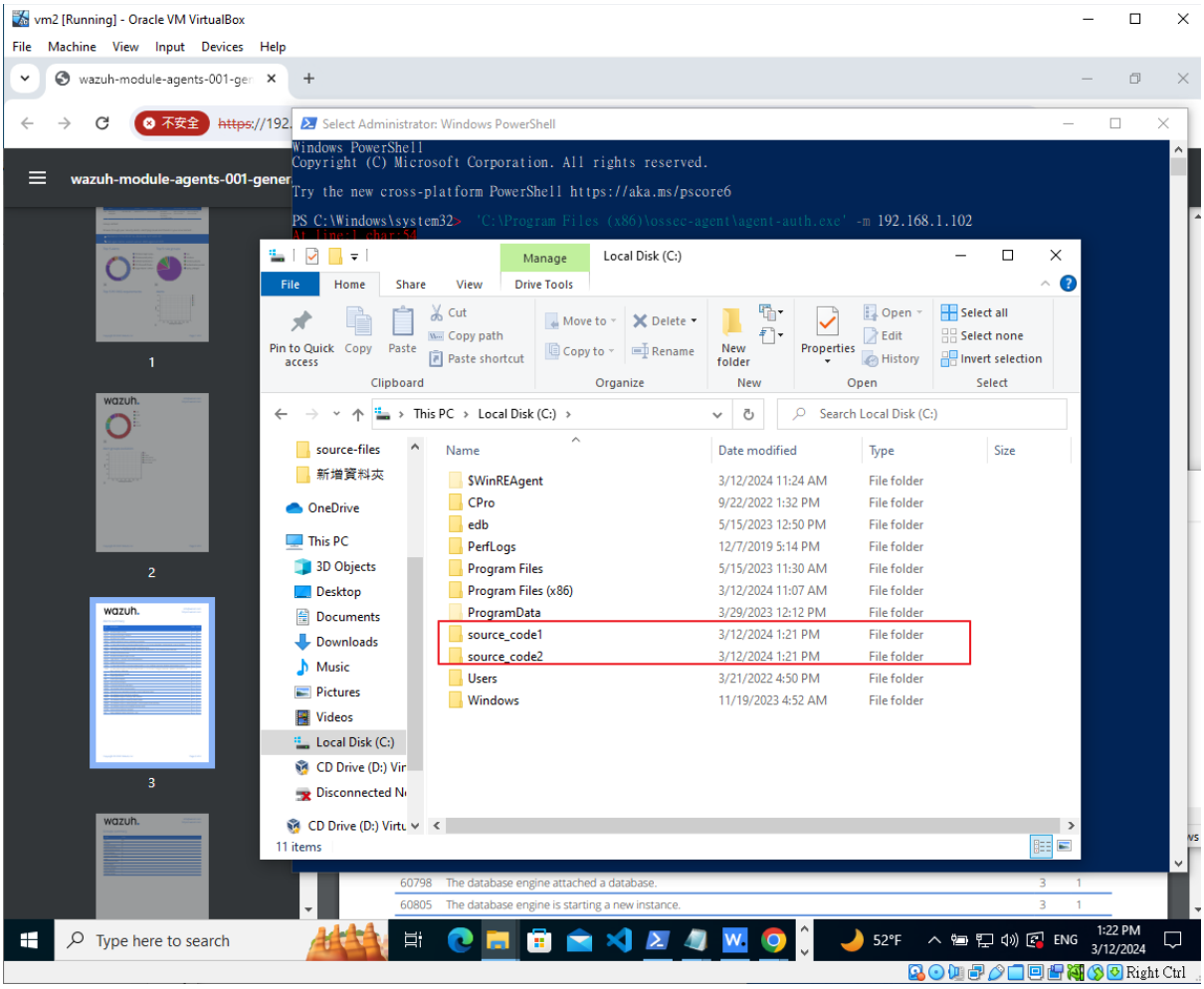
  Open the authentication failure logs in the Wazuh dashboard -> ‘generate report’. Go to ‘Management >’Reporting’. Here will be the report that records the authentication failure.


vm2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wazuh - Wazuh
不安全 https://192.168.1.102/app/wazuh#/manager/?tab=reporting
wazuh. / Management / Reporting
Reporting
Refresh
From here you can check all your reports.
Search...
File
Size
Created
Download report
wazuh-module-agents-001-general-1710216069.pdf
94.44KB
Mar 12, 2024 @ 12:01:11.839
Rows per page: 10
1
Type here to search
ENG
12:02 PM
3/12/2024
Right Ctrl



- Task 5 – Setting Up Wazuh File Integrity Monitoring

  In this task, it would need to create two folders that are monitoring targets. First, create two folders, “source_code1” and "source_code2,” in C Drive.

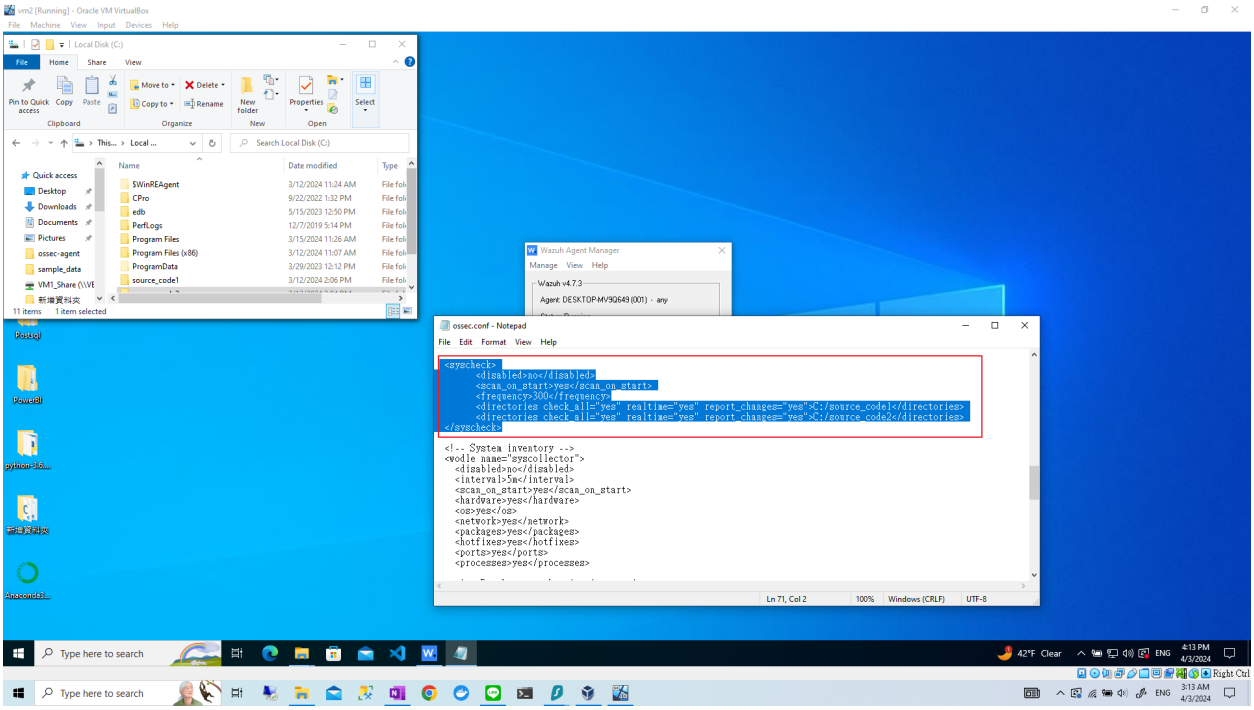


Second, go to Wazuh Agent Manager -> ‘View’ -> ‘View Config’.
Then, edit the config file. Delete the commands under <! -- File integrity monitoring -->. starting from <syscheck> to </syscheck>. [Ensure that you delete the commands in-between <! -- File integrity monitoring --> and <! – System Inventory -->].

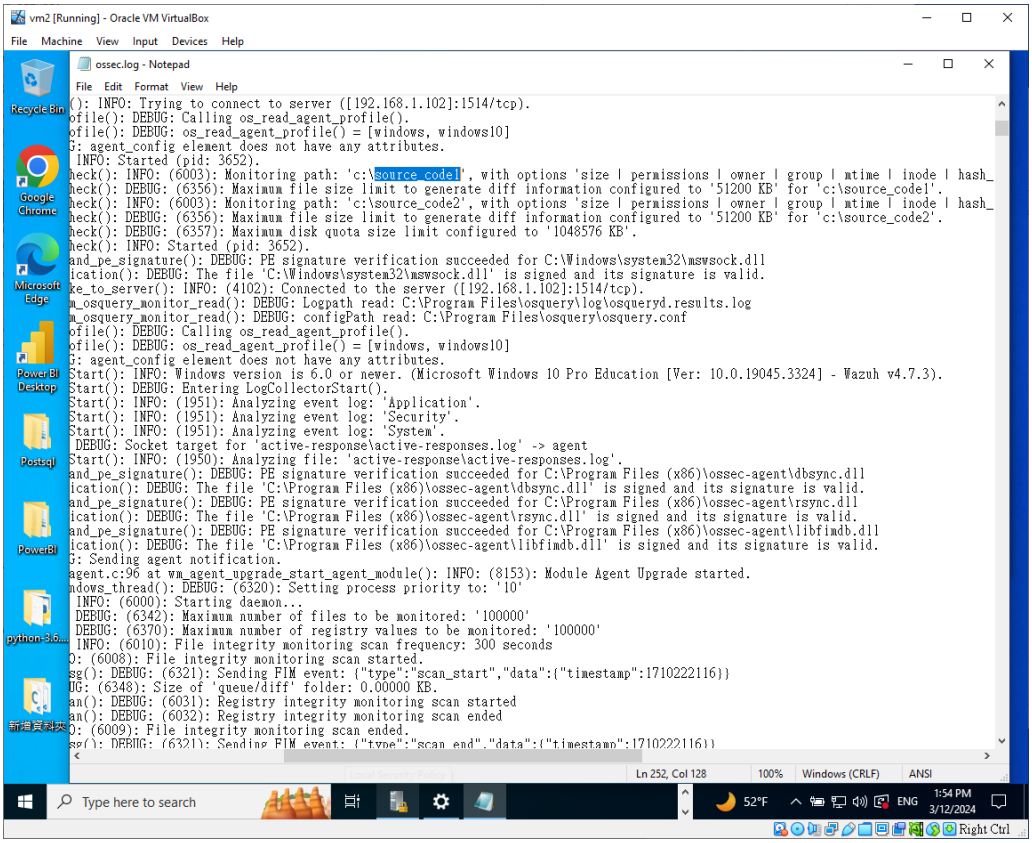
After deleting the default file integrity monitoring command, paste/type the below command under “<!-- File integrity monitoring -->”.

<syscheck>
<disabled>no</disabled>
<scan_on_start>yes</scan_on_start>
<frequency>300</frequency>
<directories check_all="yes" realtime="yes" report_changes="yes">C:/source_code1</directories> <directories check_all="yes" realtime="yes" report_changes="yes"> C:/source_code2</directories>

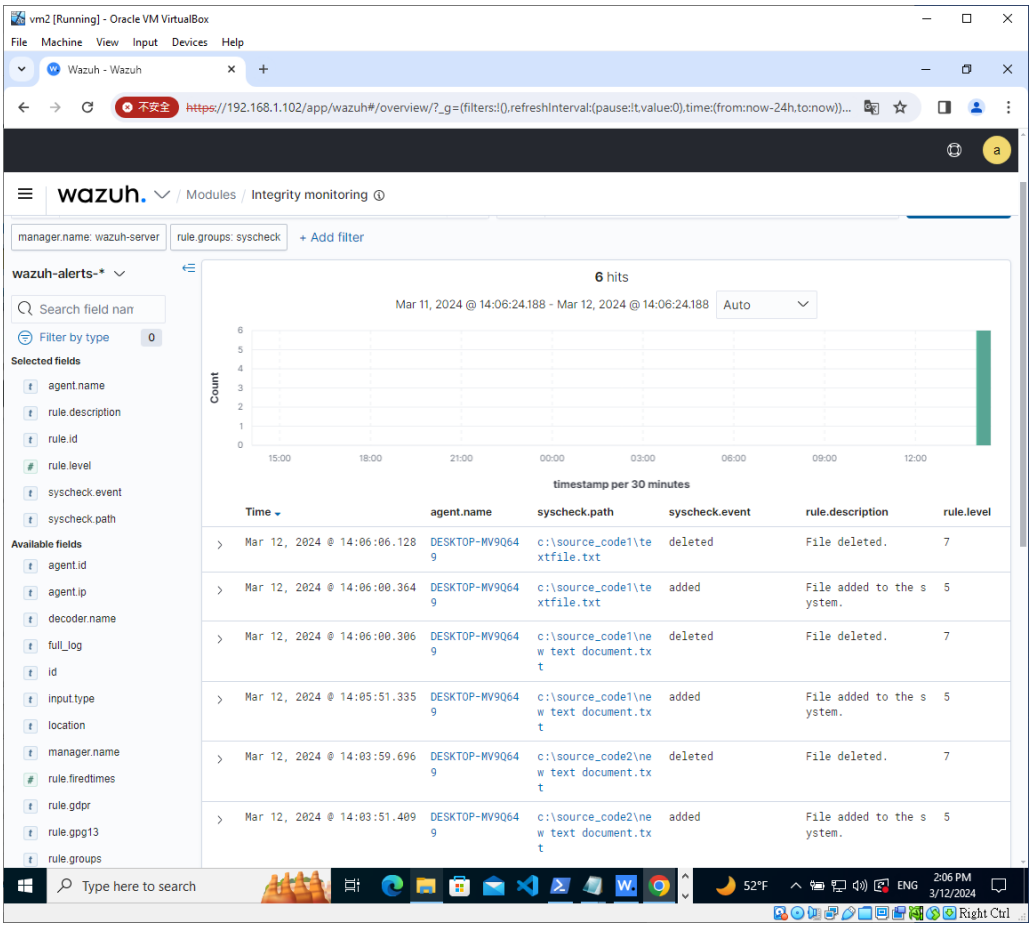
</syscheck>



Third, save the ‘View Config’, then go to ‘View Logs’. Check if the file is monitored.

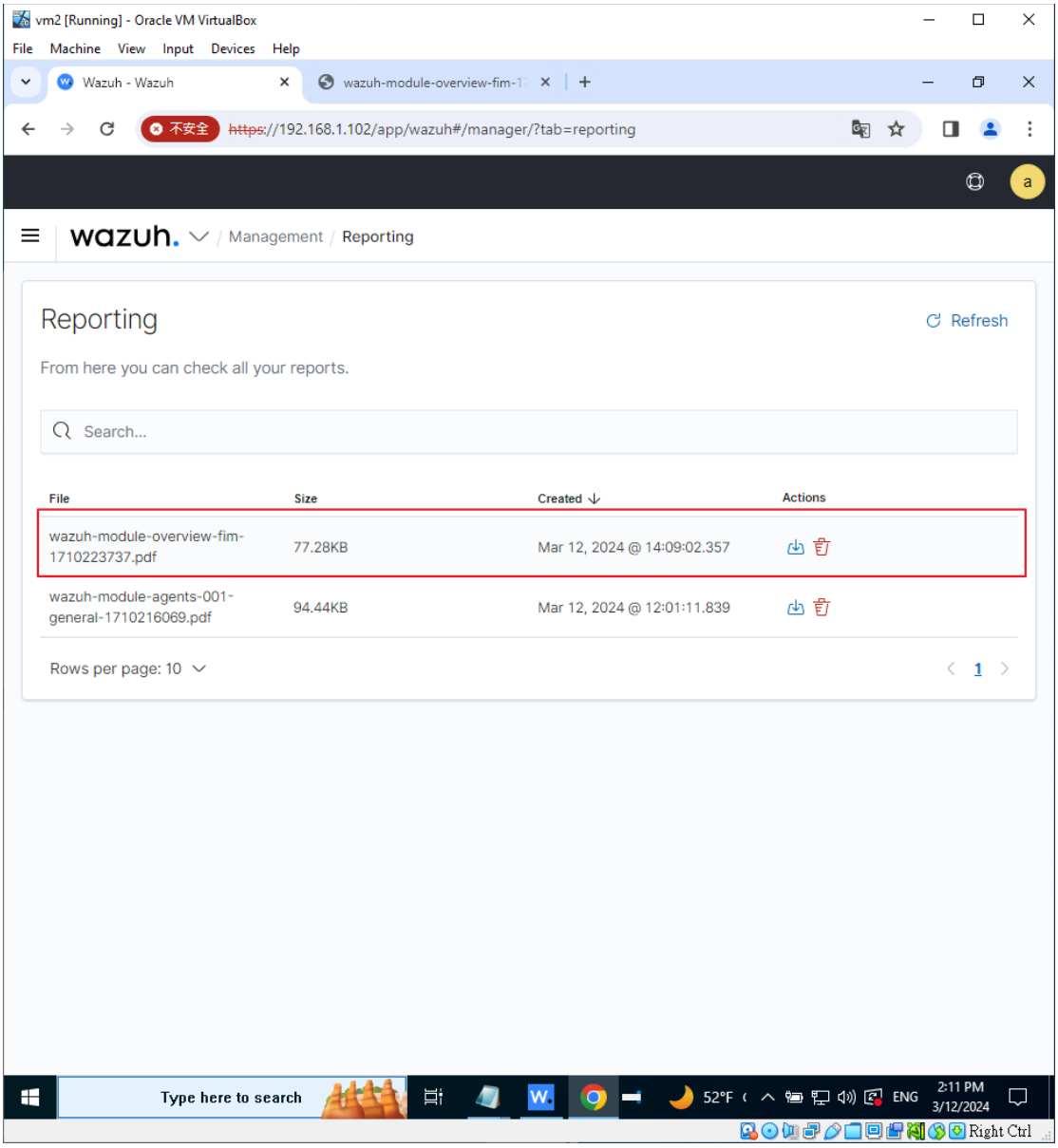


Last, go to the Wazuh dashboard and click on Integrity Monitoring. Here, it shows the operation of the folders'source_code1'' and'source_code2'.



- Task 6 – Generating Report for File Integrity Management

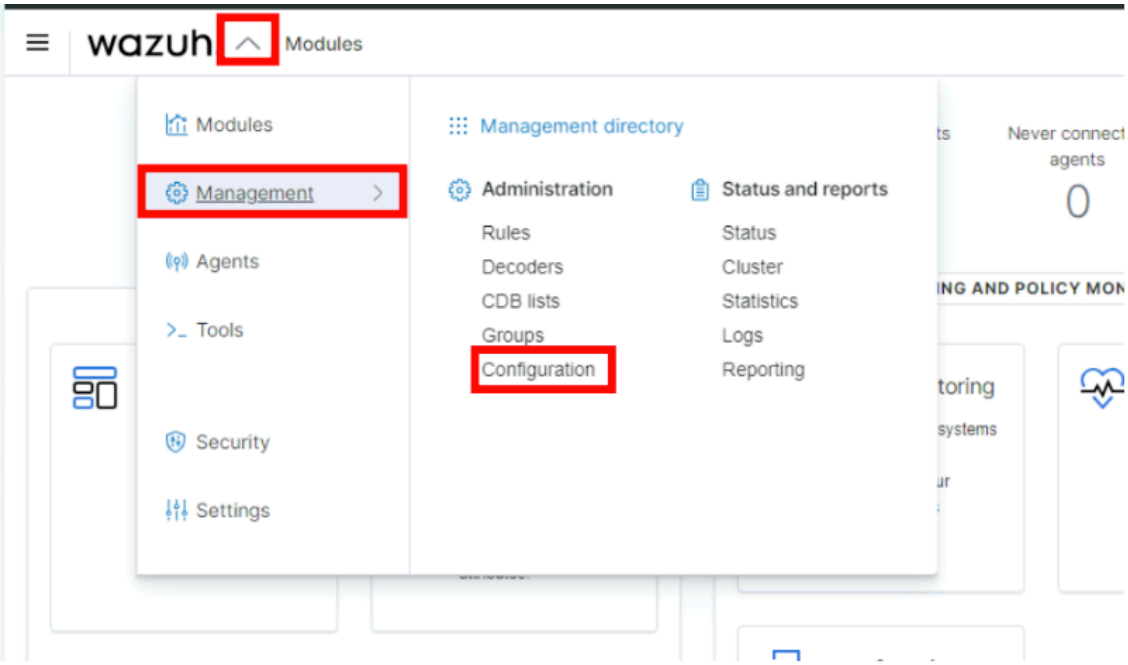
In this task, it is same as the task4. Open the Wazuh dashboard ->‘Integrity Monitoring’ ->’ Generate Report’.



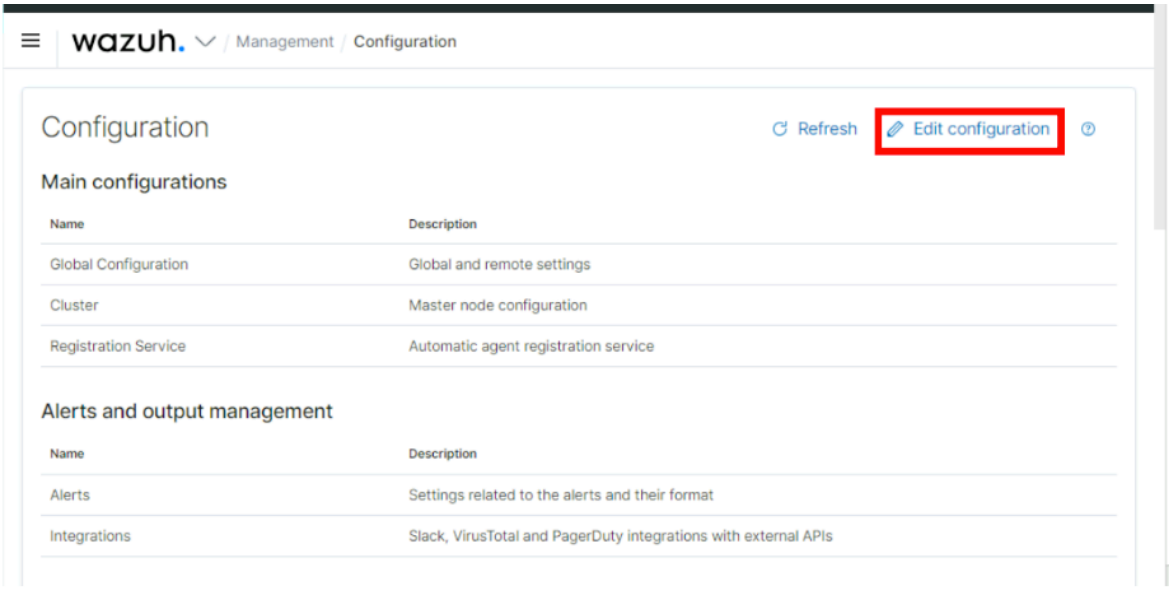
- Task 7 – Detecting Vulnerabilities in Windows Machine.

In this task, it would show how to use Wazuh to detect vulnerabilities in Windows machines.

First, open the Wazuh dashboard. Click on -> ‘Management’_>’ Configuration’.

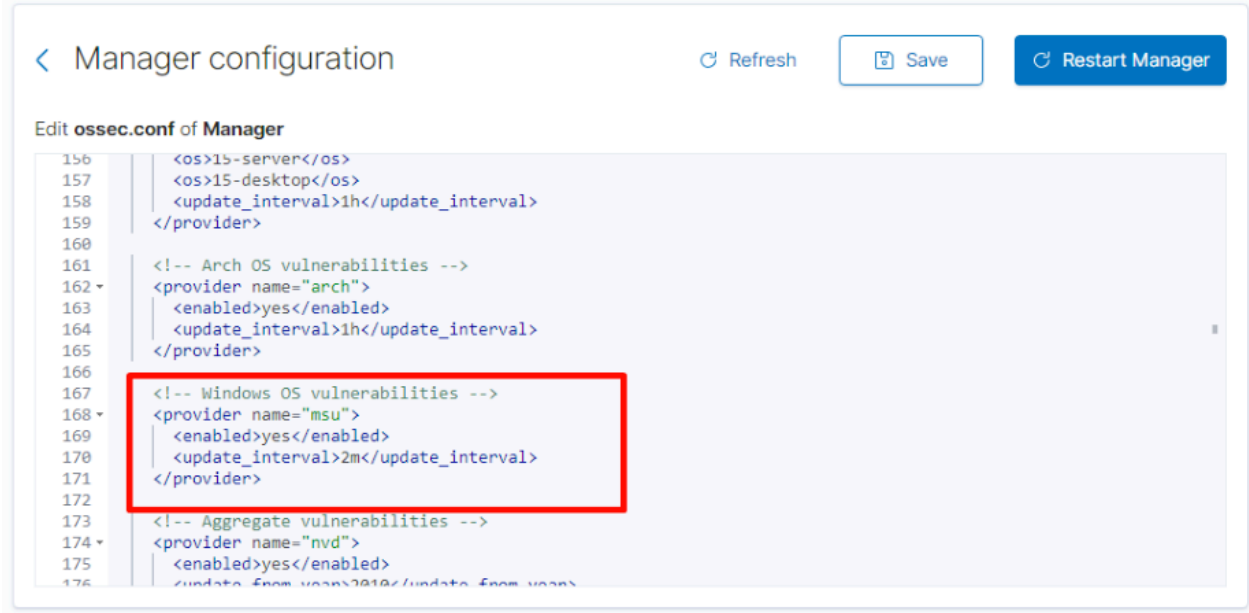


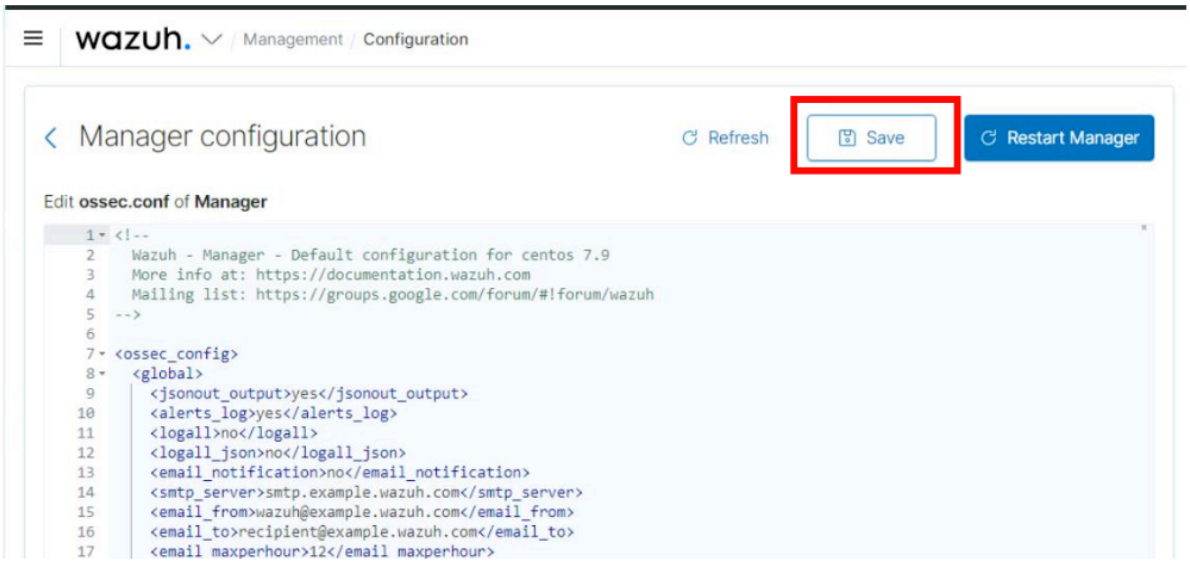
Second, Click on “Edit Configuration”.



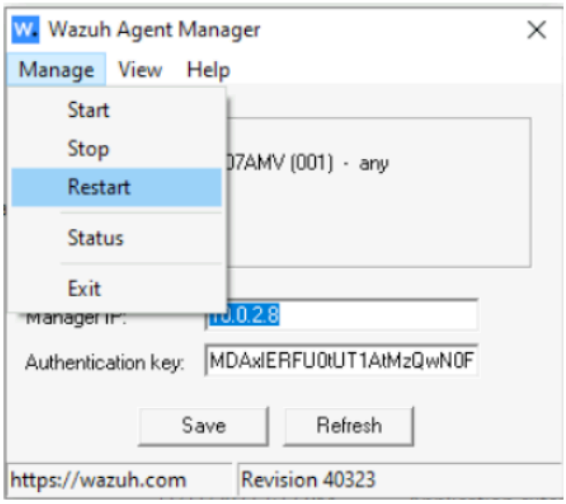
Third, edit the configuration. After edit, save the file.


Manager configuration
Refresh
Save
Restart Manager
Edit ossec.conf of Manager
<scan_on_start>yes</scan_on_start>
<interval>12h</interval>
<skip_nfs>yes</skip_nfs>
</sca>
<vulnerability-detector>
<enabled>yes</enabled>
<interval>2m</interval>
<min_full_scan_interval>5m</min_full_scan_interval>
<run_on_start>yes</run_on_start>
<!-- Ubuntu OS vulnerabilities -->
<provider name="canonical">
<enabled>yes</enabled>
<os>trusty</os>
<os>xenial</os>
<os>bionic</os>
<os>focal</os>
<os>jammy</os>
<update_interval>1h</update_interval>

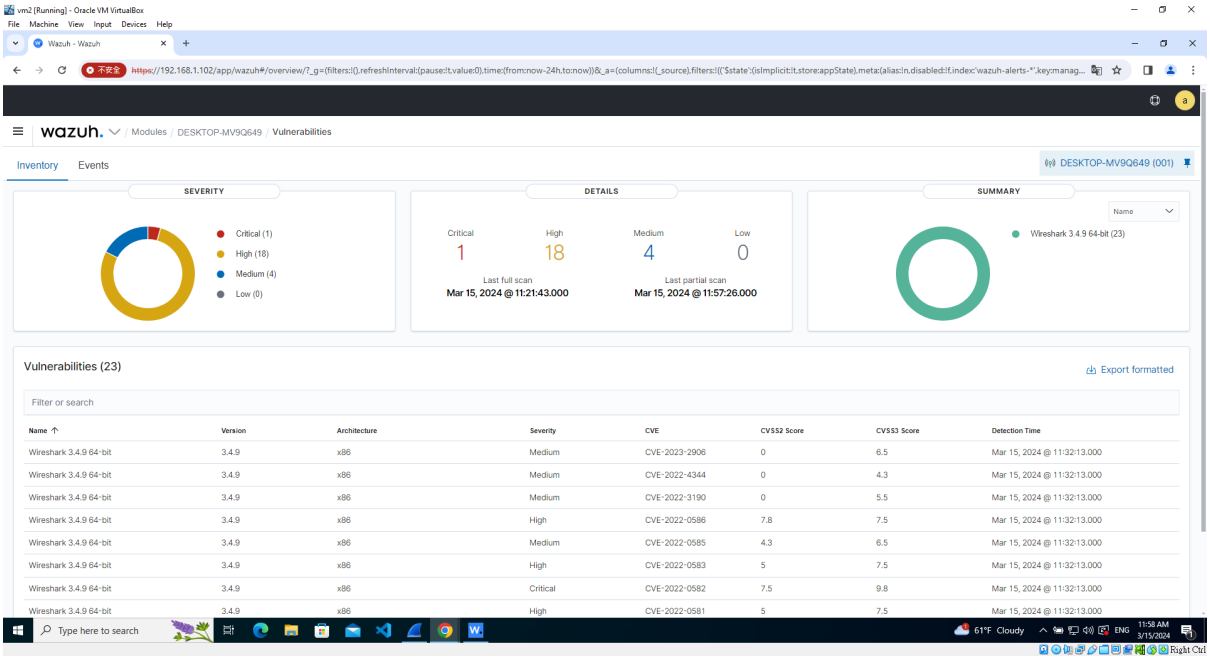

Manager configuration
Refresh
Save
Restart Manager
Edit ossec.conf of Manager
<os>15-server</os>
<os>15-desktop</os>
<update_interval>1h</update_interval>
</provider>
<!-- Arch OS vulnerabilities -->
<provider name="arch">
<enabled>yes</enabled>
<update_interval>1h</update_interval>
</provider>
<!-- Windows OS vulnerabilities -->
<provider name="msu">
<enabled>yes</enabled>
<update_interval>2m</update_interval>
</provider>
<!-- Aggregate vulnerabilities -->
<provider name="nvd">
<enabled>yes</enabled>



Then, restart the service.



Last, go to Wazuh dashboard -> ‘Vulnerabilities’. Here are the detection of vulnerabilities of the Windows machine.



- Task 8 – Analyzing the Vulnerability Dashboard

The Wazuh Vulnerability Dashboard indicates a total of 23 vulnerabilities. One of them is critical, 14 are high-level vulnerabilities, and four are medium-level vulnerabilities. There is no low level of vulnerability. Furthermore, Wireshark affects the top five high-security vulnerabilities.
At the same time, finding fixes and recommendations for vulnerabilities is crucial. Here are the fixes and advice from the NIST and Wireshark official websites.

- CVE2022-0586:
  https://nvd.nist.gov/vuln/detail/CVE-2022-0586
- CVE-2022-0583:
  https://nvd.nist.gov/vuln/detail/CVE-2022-0583
  https://www.wireshark.org/security/wnpa-sec-2022-03.html
- CVE-2022-0581:
  https://nvd.nist.gov/vuln/detail/CVE-2022-0581
  https://www.wireshark.org/security/wnpa-sec-2022-05.html
- CVE-2021-4190:
  https://nvd.nist.gov/vuln/detail/CVE-2021-4190
- CVE-2021-4186
  https://nvd.nist.gov/vuln/detail/CVE-2021-4186

https://www.wireshark.org/security/wnpa-sec-2021-16.html

Analysis:

During this capstone exercise, two reports were created in overall, one by task4 and the other by task6. Task 4 is a security events report that displays the target IP, the operating system version, and the version of the Wazuh server being utilized. Next, the report provides a concise overview of the warnings. The top three notifications in this example are 'Windows login success', 'Windows audit policy updated', and 'Windows User Logoff'. They have been recorded 19, 15, and 4 times. At the same time, this report also illustrates the evolution of alert groups. The most frequent sequence of elements is 'sca', which occurs 396 times.

Task 6 includes an integrity monitoring report. It displays notifications for file changes, such as rights, content, ownership, and attributes. Thus, the second section of this report displays the top three FIM rules, which include file uploaded to the system and file removed.

In addition, a dashboard was produced when the vulnerability analysis work was completed. There are a total of 23 vulnerabilities throughout the attack.

Technical Challenges:

In this technical capstone practice, I faced two main technical challenges.

- Insufficient RAM on the Linux computer prevents the Wazuh-indexer service from working properly.
First, I created a virtual Linux computer with a two-core CPU and two gigabytes of RAM. However, the service would terminate after the machine had run for a time. I checked

the RAM utilization and discovered that it had reached 98%. Thus, I changed the settings to 2 cores and 4 GB of RAM, which resolved the problem.

- Cannot get the vulnerability.
After resolving the prior problem, I was still stuck on task 7 since the system was unable to discover any vulnerabilities throughout the night. Therefore, I endeavored to install Wireshark to monitor network traffic and identify any suspicious activity or anomalous behavior that could potentially stem from system vulnerabilities. After installing Wireshark, I was able to find the vulnerability and overcome the task.

Learnings from Capstone:

This capstone project covers several significant trainings:
- To learn how to set up a virtual environment using a Linux machine and a Windows operating system. In addition, configure internal networking to link two VMs to each other.
- In this project, I learned how to set up Wazuh, an open source SIEM, as well as how to do log analysis, file integrity monitoring, and vulnerability detection. Knowing the tool may help strengthen the organization's or industry's cyber security posture.